DCI/IC 77-6369
19 October 1977

MEMORANDUM FOR: Members, Intelligence Definitions
Working Group

FROM: [redacted] STAT
Office of Policy and Planning
Intelligence Community Staff

SUBJECT: Minutes of Definitions Working Group Meeting

1. A summary of the meeting held on 18 October 1977 of the Intelligence Definitions Working Group is attached for your information. Also attached is the revised list of terms requested by Senator Huddleston of the Senate Select Committee on Intelligence.

2. Draft definitions have been received from Air Force, DIA, State, DCI Security Committee, and ICS/HRC, and they are included for your review. We will begin discussion of these definitions at our next meeting, scheduled for 0930, Wednesday 26 October 1977, CHB, Room 5S09. [redacted] STAT

Attachments
As Stated

MINUTES OF THE INTELLIGENCE
DEFINITIONS WORKING GROUP

18 October 1977

1. [redacted] opened the meeting by emphasizing the necessity of completing the review and discussion of definitions of the 26 intelligence terms requested by Senator Huddleston. Copies of the seven terms discussed at the 13 October 1977 meeting were distributed to the participants and attention then focused on the remaining 19 terms.

2. With the single exception of the definition of the term "International Terrorist Activities," the Group arrived at a consensus on the definitions of the remaining terms requested by Senator Huddleston. The Treasury representative requested that language similar to that found in the draft Executive Order referring to "protectees of the Secret Service or Department of State" be included in the definition. The Group did not accept this inclusion as it would necessitate adding multiple lists of other categories of people covered or not covered and the draft definition was thought to be broad enough to accommodate Treasury's interests. The Chairman stated that he would include Treasury's recommendation in his cover memorandum forwarding the definitions to [redacted] ICS, and [redacted] CIA/OLC, the primary action officers for this matter.

3. The review and discussion of the 26 terms was concluded by the Group's agreement that the use of the word "Intelligence" in the title of certain terms and the use of the word "Information" in their associated definitions necessitated the term being annotated as a colloquial expression. These terms are COMINT, ELINT, FISINT, and SIGINT.

4. Inputs from the participants containing their draft definitions of terms assigned from the composite list of intelligence terms will be disseminated and discussed at the next meeting which is scheduled for 0930, Wednesday, 26 October 1977, CHB, Room 5S0[redacted]

[redacted]
Office of Policy and Planning
Intelligence Community Staff

DEFINITIONS WORKING GROUP
18 October 1977

STAT [redacted] USA
Chairman

NAME	ORGANIZATION	PHONE
STAT [redacted]	NFAC	STAT [redacted]
Major Jack Wolfe, USA	Army/OACSI	695-4469
STAT [redacted]	NSA	688-6527
Mr. William Kenworthey, Jr.	IHC	688-7608
Capt. L. D. Dahl, USN	State/INR	632-9032
Mr. R. P. Watson	FBI	324-4583
Mr. Lawrence McWilliams	FBI	324-4591
STAT [redacted]	DIA	695-6669
Mr. Arthur Long	Treasury	566-5988
Mr. Lee Martin	DoE	376-1748
STAT [redacted]	CIA	[redacted]
	ICS (OPEI)	
	ICS (OPP)	

DEFINITIONS OF INTELLIGENCE TERMS

INTELLIGENCE: A generic term which includes foreign intelligence and foreign counterintelligence. (See below.)

INTELLIGENCE ACTIVITIES: A generic term used to describe the efforts and endeavors undertaken by the departments, agencies, and elements comprising the Intelligence Community.

FOREIGN INTELLIGENCE (FI): The product of collection, processing, and analysis of foreign intelligence information relating to the national security, to the foreign relations or economic interests of the United States by a government agency that is assigned an intelligence mission.

FOREIGN COUNTERINTELLIGENCE: Intelligence activity, with its resultant product, devoted to countering the effectiveness of foreign intelligence activities and undertaken to protect the security of the United States, its personnel, information and installations against espionage, sabotage, and terrorism. Foreign counterintelligence does not include personnel, physical, document, or communications security programs.

TACTICAL INTELLIGENCE: That intelligence required by military commanders in the field to maintain the readiness of operating forces for combat operations and to support the planning and conduct of military operations under combat conditions.

INTERNATIONAL TERRORIST ACTIVITIES: Terrorism is the calculated use of violence, or the threat of violence, to attain political goals through fear, intimidation or coercion. It usually involves a criminal act, often symbolic in nature, and is intended to influence an audience beyond the immediate victims. International terrorism is terrorism transcending national boundaries in the carrying out of the act, the purpose of the act, the nationalities of the victims, or the resolution of the incident. These acts are usually designed to attract wide publicity in order to focus attention on the existence, cause, or demands of the perpetrators.

DEPARTMENT(AL) INTELLIGENCE: Foreign Intelligence produced and used within a governmental department or agency in order to meet unique requirements of the department or agency mission.

INTELLIGENCE-RELATED ACTIVITIES: Those military activities, specifically excluded from the Consolidated Defense Intelligence Program, which respond to operational commanders' tasking for time-sensitive information on foreign activities; respond to national Intelligence Community advisory tasking of systems whose primary mission is to support operating forces; train personnel for intelligence duties; or are devoted to research and development of intelligence or related capabilities. Intelligence-related activities do not include programs which are so closely integrated with a weapon system that their primary function is to provide immediate data for targeting purposes.

COMMUNICATIONS INTELLIGENCE (COMINT): Technical and intelligence information derived from intercept of foreign communications by other than the intended recipients. COMINT does not include the monitoring of foreign public media nor the intercept of oral or written communication intercepted during the course of foreign counterintelligence investigations within the United States. (This is a colloquial term.)

ELECTRONICS INTELLIGENCE (ELINT): Technical and intelligence information derived from foreign non-communications electromagnetic radiations emanating from other than atomic detonation or radioactive sources. (This is a colloquial term.)

FOREIGN INSTRUMENTATION SIGNALS INTELLIGENCE (FISINT): Information derived from the collection and processing of foreign telemetry, beaconry, and associated signals. (This is a colloquial term.)

SIGNALS INTELLIGENCE (SIGINT): A category of intelligence information comprising all Communications Intelligence, Electronics Intelligence, and Foreign Instrumentation Signals Intelligence, either individually or in combination, including as well non-imagery infra-red and coherent light signals. (This is a colloquial term.)

NON-COMMUNICATIONS EMANATIONS: That class of radiations which are emitted intentionally or unintentionally by electrical or electronic equipments for purposes other than communications, e.g., by radars, navigational aids, jammers, or remote control systems.

UNITED STATES SIGNALS INTELLIGENCE SYSTEM: An entity that is comprised of the National Security Agency (including assigned military personnel); those elements of the military departments and the Central Intelligence Agency performing Signals Intelligence activities; and those elements of any other department or agency which may from time to time be authorized by the National Security Council to perform Signals Intelligence activities during the time when such elements are so authorized.

COMMUNICATIONS SECURITY (COMSEC): The protection resulting from the application of any measures taken to deny unauthorized persons information of value which might be derived from telecommunications or to ensure the authenticity of such telecommunications.

TRANSMISSION SECURITY (TRANSSEC): The component of Communications Security which results from all measures designed to protect transmissions from interception and from exploitation by means other than cryptanalysis.

EMISSION SECURITY (EMSEC): The component of Communications Security which results from all measures taken to deny to unauthorized persons information of value which might be derived from interception and analysis of compromising emanations from crypto-equipment and telecommunications systems.

PHYSICAL SECURITY: Physical measures--such as safes, vaults, perimeter barriers, guard systems, alarms and access controls--designed to safeguard installations against damage, disruption or unauthorized entry; information or material against unauthorized access or theft; and specified personnel against harm.

PERSONNEL SECURITY: The means or procedures, such as selective investigations, record checks, personal interviews, supervisory controls, designed to provide reasonable assurance that persons being considered for, or granted access to, classified information are loyal and trustworthy.

CRYPTOSECURITY: The component of Communications Security that results from the provision of technically sound cryptosystems and from their proper use.

CRYPTOLOGIC ACTIVITIES: The activities and operations involved in the production of Signals Intelligence and the maintenance of Communications Security.

CRYPTOLOGY: The branch of knowledge which treats the principles of cryptography and cryptanalytics and is used to produce signals intelligence and maintain communications security.

CODE: A cryptosystem in which the cryptographic equivalents (usually called "code groups"), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plaintext elements such as words, phrases, or sentences.

CIPHER: A cryptosystem in which the cryptographic treatment (i.e., the method for transforming plain text by predetermined rules to obscure or conceal its meaning) is applied to plaintext elements (such as letters, digits, polygraphs or bits) which either have no intrinsic meaning or are treated without regard to their meaning (e.g., if the element is a natural-language word).

CRYPTOSYSTEM: All associated items of cryptomaterial (e.g., equipments and their removable components which perform cryptographic functions, operating instructions, maintenance manuals) that are used as a unit to provide a single means of encryption and decryption of plain text, so that its meaning may be concealed. (In addition, Code, Cipher, and Cryptographic System include any mechanical or electrical device or method used for the purpose of disguising, authenticating, or concealing the contents, significance, or meanings of communications.)

NATIONAL INTELLIGENCE ESTIMATES (NIEs): Thorough assessments of situations in the foreign environment that are relevant to the formulation of foreign, economic, and national security policy, and project probable future courses of action and developments. They are structured to illuminate differences of view within the Intelligence Community, and are issued by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board.

D/A

Analysis - A stage in the intelligence cycle in which information is subjected to review in order to identify significant facts and derive conclusions therefrom. JCS Pub 1

Asset (intelligence) - Any resource - person, group, relationship, instrument, installation, or supply - at the disposition of an intelligence organization for use in an operational or support role. Often used with a qualifying term such as agent asset, propaganda asset. JCS Pub 1

Clandestine

Clandestine Operation - Activities to accomplish intelligence, counter-intelligence, and other similar activities sponsored or conducted by governmental departments or agencies, in such a way as to assure secrecy or concealment. (If differs from covert operations in that emphasis is placed on concealment of the operation rather than on concealment of identity of sponsor.) JCS Pub 1

Combat Intelligence - That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. JCS Pub 1

Cover - 1. The action by land, air, or sea forces to protect by offense, defense, or threat of either or both. 2. Shelter or protection, either natural or artificial. 3. To maintain a continuous receiver watch with transmitter calibrated and available, but not necessarily available for immediate use. 4. Photographs or other recorded images which show a particular area of ground. 5. Keep fighters between force/base and

contact designated at distance stated from force/base (e.g., "cover bogey" twenty-seven to thirty miles.) 6. Protective guise used by a person, organization, or installation to prevent identification with clandestine activities. JCS Pub 1

Covert Operations - Operations which are so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. They differ from clandestine operations in that emphasis is placed on concealment of identity of sponsor rather than on concealment of operation.

Deception - Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. JCS Pub 1

Defense Intelligence Community - Refers to DIA, NSA and the Military Services Intelligence offices including DoD collectors of specialized intelligence through reconnaissance programs.

Department(al) Intelligence - Intelligence which any department or agency of the Federal Government requires to execute its own mission.

Espionage - Actions directed toward the acquisition of information through clandestine operations. JCS Pub 1

Sabotage - An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by wilfully injurying or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources. JCS Pub 1

Essential Elements of Information - The critical items of information regarding the enemy and his environment needed by the commander by a particular time, to relate with other available information and intelligence in order to assist him in reaching a logical decision. JCS Pub 1

Evasion and Escape - The procedures and operations whereby military personnel and other selected individuals are enabled to emerge from an enemy - held or hostile area to areas under friendly control. JCS Pub 1

Evasion and Escape Intelligence - Processed information prepared to assist personnel to escape if captured by the enemy or to evade capture if lost in enemy-dominated territory. JCS Pub 1

Integration - A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. JCS Pub 1

Intelligence Cycle - The steps by which information is converted into intelligence and made available to users. There are five steps in the cycle:

a. planning and direction - Determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection agencies, and a continuous check on the productivity of collection agencies.

b. collection - Acquisition of information and the provision of this information to processing and/or production elements.

c. processing - Conversion of collected information into a form suitable to the production of intelligence.

d. production - Conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all source

data and the preparation of intelligence products in support of known or anticipated user requirements.

e. dissemination - Conveyance of intelligence to users in a suitable form. New JCS Pub 1

Intelligence Requirement - Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. JCS Pub 1

Interdepartment(al) Intelligence - Integrated department(al) intelligence required by departments and agencies of the U.S. government for the execution of their missions but which transcends the exclusive competence of a single department or agency to produce. JCS Pub 1

Interpretation - A stage in the intelligence cycle in which the significance of information is judged in relation to the current body of knowledge. New JCS Pub 1

Joint Intelligence - Intelligence produced by elements of more than one Service of the same nation. JCS Pub 1

Nuclear Intelligence - Intelligence derived from the collection and analysis of radiation and other effects resulting from the detonation of nuclear devices or radioactive sources.

Operational Control - The authority delegated to a commander to assign missions or tasks to subordinate commands, to deploy units, to reassign forces, and to retain or delegate operational and/or tactical control as may be deemed necessary. It does not, of itself, include administrative command or logistical responsibility. May also be used to denote the forces assigned to a commander. JCS Pub 1

Operational Intelligence - Intelligence required for planning and executing all types of operations. JCS Pub 1

Order of Battle - The identification, strength, command structure and disposition of the personnel, units, and equipment of any military force. JCS Pub 1

Processing - See Intelligence Cycle

SAO - Special Activities Office - See SCI

SSO - Special Security Office - See SCI

Sensitive Compartmented Information (SCI) - All information and materials subject to special national intelligence community controls requiring restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (Recommend JCS Pub 1)

Strategic Warning - A notification that enemy-initiated hostilities may be imminint. This notification may be received from minutes to hours, to days, or longer, prior to the initiation of hostilities. JCS Pub 1

Tactical Warning - 1. A notification that the enemy has initiated hostilities. Such warning may be received anytime from the launching of the attack until it reaches its target. 2. In satellite and missile surveillance, a notification to operational command centers that a specific threat event(s) is occurring. The component elements threat events are:

Country of origin - country or countries initiating hostilities.

Event type and size - identification of the type of event and determination of the size or number of weapons.

Country under attack - determined by observing trajectory of an object and predicting its impact point.

Event time - time the hostile event occurred. JCS Pub 1

Review - To examine, inspect, and discuss in a critical manner, precedent to consideration of value.

Evaluation - In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinency, and accuracy. Appraisal is accomplished at several stages within the intelligence cycle with progressively different contexts. New JCS Pub 1

Assess - A management deliberation in which the value of information, intelligence, activity, result, or product is weighed against resource allocation or expenditures.

Radiation Intelligence - Intelligence derived from information obtained from unintentional electro-magnetic energy emanating from foreign devices to determine their function and characteristics, excluding nuclear detonations or radioactive sources.

OPEI/HRC Proposed Definitions

GUIDANCE - Information which interprets, clarifies, or expands upon previously defined intelligence needs. Consumer guidance points the way for collection managers. Collection manager guidance steers the course of field collection.

REQUIREMENT - A specific statement of information need. A specific form of guidance which is sanctioned by the resource manager and carries an implicit authorization to commit resources in collection tasking.

TASKING - The assignment or direction, by command channel, of an individual or activity to perform in a specified way for achievement of a specified end, objective, or goal.

DOWNGRADE. To change the security classification of official information from a higher to a lower level.

DECLASSIFY. To remove official information from the protective status afforded by security classification.

COMPROMISE. The exposure of classified official information or activities to persons not authorized access thereto.

SECURITY. The sum of those measures, such as physical, personnel, technical, and communications security, designed to protect official information against compromise, unauthorized disclosure or espionage; official installations against damage, disruption or unauthorized entry; and official personnel against harm or subversion.

SENSITIVE COMPARTMENTED INFORMATION. All information and materials bearing special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products for which Community systems of compartmentation have been or will be formally established.

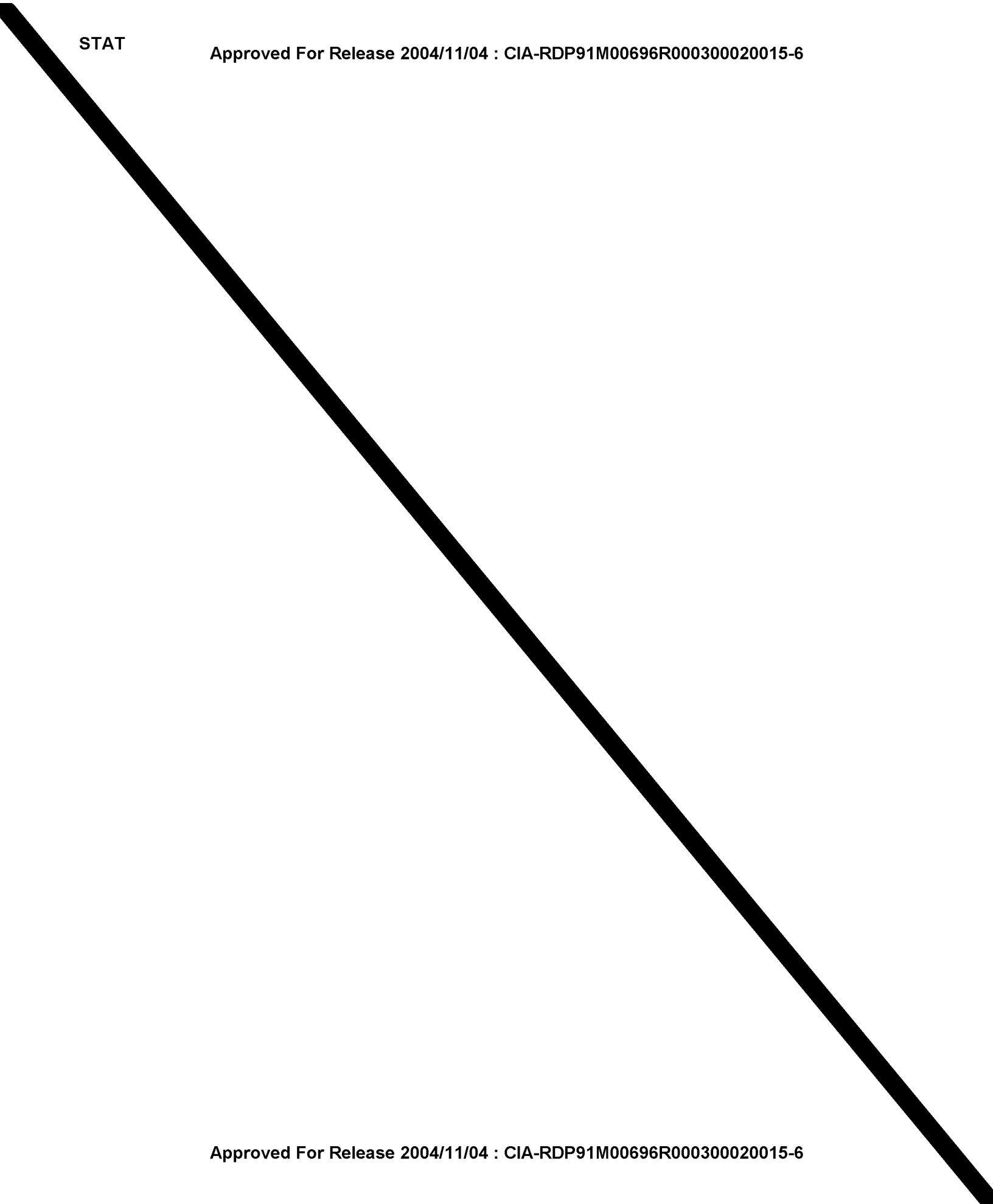
COMPUTER SECURITY. The means and procedures to provide protection of classified foreign intelligence involving sensitive intelligence sources and methods, processed and/or stored in Automated Data Processing (ADP) systems and networks.

COMPARTMENTATION. Formal systems of restricted access established and/or managed by the DCI to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs.

DECOMPARTMENTATION. The removal of information from a compartmentation system without attempting to conceal the source.

SANITIZATION. The concealment of sensitive intelligence sources, methods, and analytical procedures to permit dissemination of information outside of compartmentation systems.

CLASSIFICATION AUTHORITY. Those officials within the Executive Branch who are concerned with matters of national security and have been authorized by the President, his designees, or Executive Order, to originally classify information or material under E.O. 11652.



Approved For Release 2004/11/04 : CIA-RDP91M00696R000300020015-6

STATE

END PRODUCT

Synonymous with the term finished intelligence. Although an intelligence field activity or source may report everything collected regarding a particular subject, it remains a product, or raw information, until it has been subjected to the full intelligence processing cycle.

Open-Source Intelligence (Information): A generic term describing that information which has inherent intelligence value which is derived from the mass of data available to the general public. This information is available free of encumberances such as security classification or any restrictive caveats.

Approved For Release 2004/11/04 : CIA-RDP91M00696R000300020015-6